Software Engineering Institute

Integrating the Master of Software Assurance Reference Curriculum into the Model Curriculum and Guidelines for Graduate Degree Programs in Information Systems

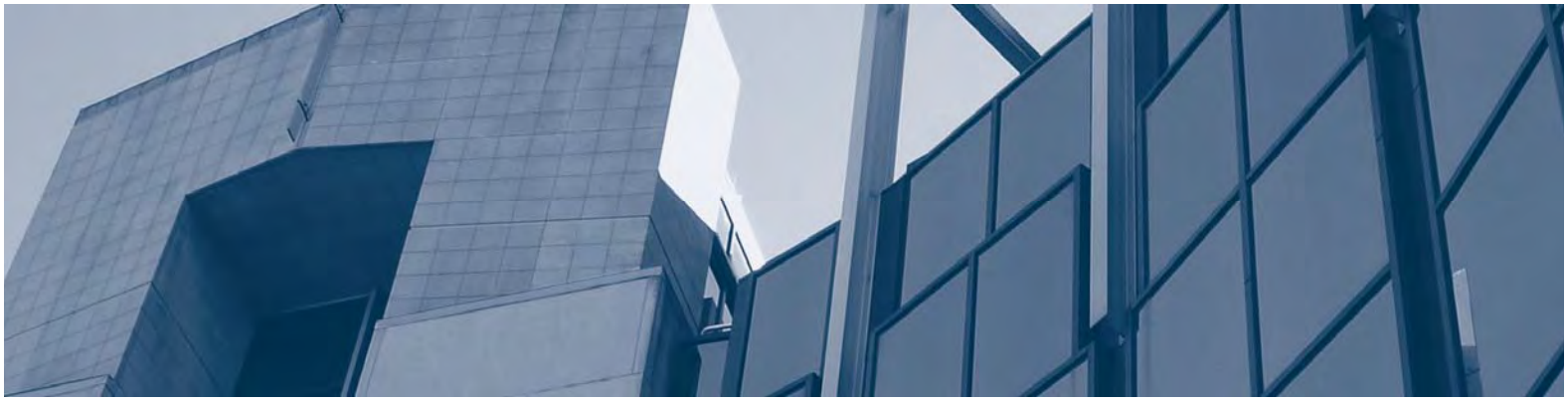
Dan Shoemaker, University of Detroit Mercy
Nancy R. Mead, Software Engineering Institute
Jeff Ingalsbe, University of Detroit Mercy

February 2011

TECHNICAL NOTE
CMU/SEI-2011-TN-004

CERT® Program
Unlimited distribution subject to the copyright.

http://www.sei.cmu.edu



Carnegie Mellon

This report was prepared for the

SEI Administrative Agent
ESC/XPK
5 Eglin Street
Hanscom AFB, MA 01731-2100

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

This work is sponsored by the U.S. Department of Defense. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

Copyright 2011 Carnegie Mellon University.

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this report is not intended in any way to infringe on the rights of the trademark holder.

Internal use. Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

External use. This document may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

For information about SEI publications, please visit the library on the SEI website (www.sei.cmu.edu/library).

Table of Contents

List of Tables

Acknowledgments

We are pleased to acknowledge the sponsor of the MSwA Reference Curriculum, Joe Jarzombek, Director for Software Assurance, National Cyber Security Division, Department of Homeland Security, and the contributions of our editorial staff, Paul Ruggiero and Lisa Gardner.

Abstract

Training personnel to assure the secure development, sustainment, and acquisition of software code is a national priority. However, in the secure software domain, there is no single, commonly accepted point of reference to direct software assurance education and training. In response to this problem, the CERT® Program at Carnegie Mellon University's Software Engineering Institute recently led the development of a Master of Software Assurance (MSwA) Reference Curriculum. This report examines how the recommendations of the MSwA Reference Curriculum might be integrated into the model curriculum recommendations for a Master of Science in Information Systems (MSIS). This integration is important because IS programs constitute a key portion of computer education programs in the United States. The report describes the content areas of the MSIS curriculum that appear to be most relevant to secure software assurance practice. It also details the places in the current MSIS curriculum model where recommendations of the MSwA Reference Curriculum appear to fit. In addition the report explains how those recommendations can be integrated into a conventional MSIS curriculum and provides an example of an existing MSIS curriculum that embodies them.

1 Introduction

1.1 The Model Curriculum and Guidelines for Graduate Degree Programs in Information Systems[1]

The *Model Curriculum and Guidelines for Graduate Degree Programs in Information Systems* (MSIS) 2006 is the latest product of a project that has been conducted for nearly 40 years [Gorgone 2006]. Various organizations affiliated with the project have developed specifications for the teaching of information systems content in higher education, including the Association for Information Systems (AIS) and the Association for Computing Machinery (ACM). Both of these organizations represent a significant constituency in professional computing.

The AIS and ACM are global in their scope and incorporate contributions from both the professional and academic computing communities. The AIS, which was organized in 1994, comprises faculty members in information systems (IS). The most recent MSIS curriculum produced by AIS, MSIS 2006, presents a model curriculum for graduate degree education in information systems at the master's level. Given the typical placement of IS programs in business schools, it needs to be understood that MSIS 2006 contains recommendations for an entire curriculum, not a concentration or option in an MBA program. In that respect, the sponsoring associations and the academic community generally agree that the MSIS 2006 curricular recommendations define the knowledge and skills required for IS professionals [Gorgone 2006].

The recommendations in MSIS 2006 can serve as a guideline from which individual institutions can tailor their own curriculum. The sponsoring associations do not expect that each institution will follow the model curriculum precisely. Instead the MSIS 2006 recommendations are meant to facilitate the creation of a comprehensive master's level IS program. In addition to recommendations about the curricular framework and general content, MSIS 2006 also provides specific examples of content for each course. At this point, over 200 master's degree programs worldwide utilize the recommendations of MSIS 2006.

The sponsoring associations of the MSIS 2006 all accept that no single IS degree program can present every fact or every process that graduates might need. Moreover given the rapid development of technology, university-level IS curricula need to be frequently updated to remain effective. Therefore MSIS 2006 recommends a basic and coherent set of fundamental concepts that will undergird productive professional work and provide a basis for lifelong learning.

According to the sponsoring organizations of MSIS 2006, when universities and other graduate-level educational institutions develop curricula, they normally incorporate four considerations [Gorgone 2006]:

- the common body of knowledge (CBK) that a graduate is expected to know. (The aim of the CBK is to counter local requirements bias and help prepare graduates for positions in other geographic areas.)
- a program structure with suggested courses and course sequences

[1] Much of this section is summarized from Gorgone and associates [Gorgone 2006].

- the practical rationale and required resources for the program
- the practical rationale for the required investment to keep faculty members up to date with rapidly changing technology and management approaches

Accounting for these considerations helps ensure that an institution's individual courses of study are relevant to the industry that its students are preparing to enter. Demonstrating compliance with a set of such recommendations assures students and the public that the program's curricula meet a minimum standard. The existence of a single, commonly acknowledged reference curriculum is a valuable means of documenting public accountability and continued program quality [Impagliazzo 2002].

The public in general, and students in particular, want to know that their course of study subscribes to the commonly accepted best practices for the profession. Programs that can demonstrate compatibility with those practices will probably increase their degree's value in the marketplace. Thus institutions of higher education must document compliance with the principles embodied in a general curriculum standard to prove that they have met the learning requirements for a given profession. The recommendations of the MSIS 2006 can represent a single, authoritative basis for such compliance documentation. Moreover those recommendations become the single point of entry to ensure the widespread teaching of software assurance content in IS programs.

1.2 Why Software Assurance Is Important

Since 9/11, the U.S. government has been extremely interested in substantive measures to ensure the integrity of the national infrastructure. Yet it is well documented that the "Commonly used software engineering practices [within that infrastructure] permit dangerous defects" [Goertzel 2007]. This is the case because "commercial software engineering lacks the rigorous controls needed to [ensure defect-free] products at acceptable cost" [PITAC 2005]. As a result, the National Strategy to Secure Cyberspace contains a specific priority to create a national cyberspace awareness and training program [DHS 2003].

That priority recognizes two of the barriers to the improvement of cybersecurity as "a lack of familiarity, knowledge, and understanding of the issues" and "an inability to find sufficient numbers of adequately trained ... personnel to create and manage secure systems" [DHS 2003]. One of the priority's major initiatives is to "foster adequate training and education programs to support the Nation's cybersecurity needs" [DHS 2003]. In order to support this goal, we need to guarantee that software assurance practices are integrated into the day-to-day activities of the overall workforce [Mead 2008].

Although we know how to assure the secure development, sustainment, and acquisition of software code, software assurance knowledge is not making its way into the profession in any organized fashion. The dilemma with software assurance is that its knowledge elements appear to cut across many disciplines, rather than being focused in a few. In essence, the knowledge base for software assurance spans a range of traditional studies [Mead 2008]. These include such dissimilar areas as "software engineering, systems engineering, information systems security engineering, safety, security, testing, information assurance, law and project management" [Redwine 2008]. Consequently, potentially meaningful software assurance content appears in many different places, and educators in conventional settings teach it in many different ways [Redwine 2006].

These settings—formally constituted education, training, and awareness programs—are the traditional means of disseminating new knowledge [Mead 2008, Bishop 2006]. Dissemination is important. The National Strategy recognizes this fact in Action Recommendation 2-14, which states that "DHS will facilitate a national public-private effort to promulgate best practices and methodologies that promote integrity, security, and reliability in software code development, including processes and procedures that diminish the possibilities of erroneous code, malicious code, or trap doors that could be introduced during development." [DHS 2003]. In the secure software domain, however, there is no single, commonly accepted point of reference to "guide the development and integration [into curricula] of education and training content relevant to software assurance" [Redwine 2008]. It is clearly unacceptable to approach the teaching and learning process without such a reference point. For that reason, the software community generally recognizes that it is important to provide a consolidated view of the body of knowledge for secure software assurance [Mead 2008, Redwine 2008, Bishop 2006, PITAC 2005].

The CERT program at the Software Engineering Institute (SEI) at Carnegie Mellon University recently led an important part of this effort: the organized development of a software assurance reference curriculum. The curriculum development team included technical staff from the SEI and faculty from a number of universities, both domestic and international [Mead 2010]. The involvement of the SEI is particularly important because much of the body of knowledge in secure software assurance is derived from software engineering principles and practices [Redwine 2008, Redwine 2006, Abran 2004]. The SEI is generally recognized as the preeminent source of new knowledge in this field. The Software Assurance Reference Curriculum Project developed at the SEI specifies an authoritative curricular framework, inherent topics, and the prerequisite knowledge and skills to ensure a properly educated software assurance professional [Mead 2010].

One of the outcomes of this project was the report *Software Assurance Curriculum Project Volume I: Master of Software Assurance Reference Curriculum* [Mead 2010]. It contains the reference curriculum, a glossary of terms, and the guidelines used to develop the curriculum, prerequisites, proposed outcomes, architecture, proposed curricular body of knowledge, and implementation considerations. A number of existing artifacts, including *Software Assurance: A Curriculum Guide to the Common Body of Knowledge* [Redwine 2008], the recent Graduate Software Engineering curriculum guidelines [SIT 2009], and the older *SEI Reports on Graduate Software Engineering Education* [Ford 1991, Ardis 1989]. The project team also referenced the *Guide to the Software Engineering Common Body of Knowledge* [Abran 2004] as needed to cross-reference the team's recommendations with the software engineering knowledge fundamental to software assurance. The Master of Software Assurance (MSwA) Reference Curriculum report recommends the following core body of knowledge (Table 1):

Table 1: MSwA Core Body of Knowledge [Mead 2010]

Knowledge Area	
1.Assurance Across Life Cycles	1.1. Software Life-Cycle Processes 1.1.1. New development 1.1.2. Integration, assembly, and deployment 1.1.3. Operation and evolution 1.1.4. Acquisition, supply, and service
	1.2. Software Assurance Processes and Practices 1.2.1. Process and practice assessment 1.2.2. Software assurance integration into SDLC phases
2.Risk Management	2.1. Risk Management Concepts 2.1.1. Types and classification 2.1.2. Probability, impact, severity 2.1.3. Models, processes, metrics
	2.2. Risk Management Process 2.2.1. Identification 2.2.2. Analysis 2.2.3. Planning 2.2.4. Monitoring and management
	2.3. Software Assurance Risk Management 2.3.1. Vulnerability and threat identification 2.3.2. Analysis of software assurance risks 2.3.3. Software assurance risk mitigation 2.3.4. Assessment of software assurance processes and practices
3.Assurance Assessment	3.1. Assurance Assessment Concepts 3.1.1. Baseline level of assurance; allowable tolerances, if quantitative 3.1.2. Assessment methods
	3.2. Measurement for Assessing Assurance 3.2.1. Product and process measures by life-cycle phase 3.2.2. Other performance indicators that test for the baseline, by life-cycle phase 3.2.3. Measurement processes and frameworks 3.2.4. Business survivability and operational continuity
	3.3. Assurance Assessment Process (collect and report measures that demonstrate the baseline) 3.3.1. Comparison of selected measurements to the established baseline 3.3.2. Identification of out-of-tolerance variances
4.Assurance Management	4.1. Making the Business Case for Assurance 4.1.1. Valuation and cost/benefit models, cost and loss avoidance, return on investment 4.1.2. Risk analysis 4.1.3. Compliance justification 4.1.4. Business impact/needs analysis
	4.2. Managing Assurance 4.2.1. Project management across the life cycle 4.2.2. Integration of other knowledge units
	4.3. Compliance Considerations for Assurance 4.3.1. Laws and regulations 4.3.2. Standards 4.3.3. Policies

Knowledge Area	
5. System Security Assurance	5.1. For Newly Developed and Acquired Software for Diverse Applications 5.1.1. Security and safety aspect of computer-intensive critical infrastructure 5.1.2. Potential attack methods 5.1.3. Analysis of threats to software 5.1.4. Methods of defense
	5.2. For Diverse Operational (Existing) Systems 5.2.1. Historic and potential operational attack methods 5.2.2. Analysis of threats to operational environments 5.2.3. Designing of and plan for access control, privileges, and authentication 5.2.4. Security methods for physical and personnel environments
	5.3. Ethics and Integrity in Creation, Acquisition, and Operation of Software Systems 5.3.1. Overview of ethics, code of ethics, and legal constraints 5.3.2. Computer attack case studies
6. System Functionality Assurance	6.1. Assurance Technology 6.1.1. Technology evaluation 6.1.2. Technology improvement
	6.2. Assured Software Development 6.2.1. Development methods 6.2.2. Quality attributes 6.2.3. Maintenance methods
	6.3. Assured Software Analytics 6.3.1. Systems analysis 6.3.2. Structural analysis 6.3.3. Functional analysis 6.3.4. Analysis of methods and tools 6.3.5. Testing for assurance 6.3.6. Assurance evidence
	6.4. Assurance in Acquisition 6.4.1. Assurance of acquired software 6.4.2. Assurance of software services
7. System Operational Assurance	7.1. Operational Procedures 7.1.1. Business objectives 7.1.2. Assurance procedures 7.1.3. Assurance training
	7.2. Operational Monitoring 7.2.1. Monitoring technology 7.2.2. Operational evaluation 7.2.3. Operational maintenance 7.2.4. Malware analysis
	7.3. System Control 7.3.1. Responses to adverse events 7.3.2. Business survivability

2 MSIS 2006 and the MSwA Reference Curriculum

Establishment of a new degree program is a very ambitious undertaking. It is worthwhile to consider how the recommendations of the MSwA Reference Curriculum might be integrated into the model curriculum recommendations for a Master of Science in Information Systems (MSIS) curriculum [Gorgone 2006]. Because IS programs constitute a key proportion of the computer education programs in the United States, it is important to be able to integrate the recommendations of the MSwA Reference Curriculum into the teaching of conventional topics in the IS discipline.

The IS programs in higher education have tended to be located in colleges of business rather than engineering or computer science schools. That is because the discipline evolved in the 1970s out of the emerging needs of business for computerized management information [Banker 2004]. Consequently the discipline's body of knowledge is most applicable to pragmatic business needs rather than the study of computer functioning itself, which is the domain of the more scientific fields such as computer science and software engineering [Banker 2004]. The pragmatic ties of IS programs to business have caused them to produce the bulk of the information technology (IT) workforce, and the field itself is growing at a higher rate than the "average for all occupations" [Bureau of Labor Statistics 2009].

The purpose of this section of the report is to provide the adaptation of the MSwA Reference Curriculum into the teaching of conventional topics in the IS discipline. This report will describe the content focus of the areas of the MSIS curriculum that appear to be the most relevant to secure software assurance practice. It will detail the places in the current MSIS curriculum model where the recommendations of the MSwA appear to fit. It will present a picture of how those recommendations can be integrated into a conventional MSIS curriculum. Finally it will present an example of an existing MSIS curriculum that has embodied those recommendations.

2.1 Comparison of MSIS to MSwA Recommendations

Table 2 summarizes the comparison between the recommendations of MSIS 2006 and the recommendations of the MSwA Reference Curriculum.

Table 2: Comparison of Content Areas

MSwA Recommendations	Comparable MSIS Recommendations
Assurance Across Life Cycles	Project and Change Management Fundamentals of IS
Risk Management	Analysis, Modeling, and Design
Assurance Assessment	Programming, Data, File, and Object Structures
Assurance Management	Enterprise Models Policy and Strategy
System Functionality Assurance	Not Applicable
System Operational Assurance	Not Applicable

There are two general points of difference that appear to cause the greatest divergence between the two models.

The first difference is between the prerequisite requirements. The MSwA Reference Curriculum has a rigorous set of prerequisite requirements that are characteristic of study in engineering and

science. The prerequisites are divided into three categories: computing foundations (discrete mathematics, computing fundamentals, networks and communications, programming environments, and program development), software engineering (software development life cycle, software analytics), and security engineering (security issues). The MSIS, on the other hand, has a clear business orientation. Its prerequisites fall into six general areas: the common body of knowledge for business (CBB), finite mathematics, elementary statistics, elementary computer programming, elementary economics, and elementary psychology. The mismatch between the purposes of these two curricular models is clear.

The second area of difference is the expected outcomes. Graduates of a program that is based on the recommendations of MSIS 2006 are expected to have general management and technology knowledge that includes the following abilities:

- integrate IS and business foundations
- maintain a broad business and real-world perspective
- exhibit communication, interpersonal, and team skills
- exhibit analytical and critical thinking skills
- exhibit specific skills leading to a career

Graduates from the MSwA curriculum are expected to be able to perform the following seven activities:

- assurance across the life cycle
- risk management
- assurance assessment
- assurance management
- system security assurance
- system functionality assurance
- system operational assurance

3 Detailed Integration of MSwA and MSIS Content Areas

This section presents the possible points of integration for the two reference models. The suggested points of integration will be generally structured by the MSwA content areas, using the specific content recommendations of the MSIS to detail the potential curricular locations. This section is taken directly from the MSIS course descriptions for this content area; the full text is available in MSIS 2006 [Gorgone 2006]. Discussion sections in brackets are suggestions by the authors of this report and are not part of MSIS 2006.

3.1 MSwA Content Area One – Assurance Across Life Cycles

Analogous MSIS Content Area: MSIS2006.5 Project and Change Management

Prerequisite: IS 2002.1 Fundamentals of Information Systems (undergraduate)

Catalog Description MSIS2006.5 Project and Change Management:

> *Managing projects within an organizational context, including the processes related to initiating, planning, executing, controlling, reporting, and closing a project. Project integration, scope, time, cost, quality control, and risk management. Software size and cost estimation. Assigning work to programmer and other teams. Monitoring progress. Version control. Managing the organizational change process. Identifying project champions, working with user teams, training, and documentation. The change management role of the IS specialist. The use of sourcing and external procurement; contracts and managing partner relationships.*

MSIS Objectives:

> *Students develop detailed project plans, schedules, and budgets; estimate project resources; allocate/coordinate resources; and interface with management. They are expected to learn tools and techniques of project planning and management, including the use of project management software. The course develops skills in the human and organizational implications of change including understanding the organizational change process; identifying stakeholders; assessing potential impacts of projects; and overcoming resistance, politics, and other human issues.*

Detailed Topic List:

- *Managing software / technology projects:*
  - *Project lifecycle*
  - *Project stakeholders*
  - *Project management skills (leading, communicating, negotiating, influencing, and presenting)*
  - *Project planning (definition, scope, schedule, costs, quality, resources, and risks)*
  - *Estimating software size and cost*
  - *Software work module design, assignment, and control.*
  - *Role of repository, project library, and version control*
  - *Contingency planning*

  - *Project reporting and controls (definition, scope, schedule, costs, quality, resources, and risks),*
  - *Testing and testing plans; alpha and beta.*
- *Managing organization change*
  - *The role of IS specialists as change agents*
  - *Envision change and the change process*
  - *Diagnose and conceptualize change*
  - *Deal with the challenges of implementation and understand and cope with resistance*
  - *Deal with issues of motivation, interpersonal relations, group/team dynamics, and leadership in the change process; implications of cross-organization and international teams.*
  - *Manage organizational politics*
  - *The limitations of projects as organizational change initiatives*
  - *Organizational influences on project success (culture, organizational structure, rewards, and measures)*
  - *Software project management resources and professional development such as SMI and PMI.*
  - *Additional activities required to ensure the success of IT projects (training, job redesign, communication, etc.)*
  - *Manage sourcing partners as well as define contract and relationships*
  - *Hands-on experience using project management software (e.g. Microsoft Project)*

Discussion:

Context of the course in the total curriculum: This course introduces two major, related topics into the required portion of the MS program: project management and change management. MS degree holders in information systems will inevitably be involved in the management of IS projects and, as a result, in the management of the changes that projects introduce. This course is fundamental to almost all career tracks and essential for students who undertake a practicum.

Philosophy underlying the selection of topics: Most information systems work is organized as a project rather than being department or function oriented. Therefore, it is essential for IS specialists to know how to manage projects effectively. But good project management alone is not sufficient to ensure organizational success with information systems. Work in this environment is a series of projects, which are conceived, staffed, completed, and shut down. Although IS projects are among the most challenging, being able to plan and manage any business project is an increasingly important and marketable skill. [Given the end-to-end relationship between project management and the software development life cycle, this is the course where content related to assurance across the life cycle would best fit.] *This course examines the roles, responsibilities, tools, and techniques for effective project management. A blend of theory and practice, the course addresses project organization, project planning, project execution, and project control. Some of the topics in project management section were selected from the Project Management Institute's "Project Management Body of Knowledge." … Other topics relate more closely to software engineering.*

Research shows that projects are a rather risky (i.e., failure-prone) way of attempting to create organization change. Therefore, IS specialists must understand and be able to apply

alternative ways of bringing about organization change, such as dealing with organizational politics and designing systems that are culturally compatible. Further, organizational success with information systems usually requires the fulfillment of activities that are not always performed by IS specialists, such as job retraining and the development of new measurement and reward systems. IS specialists must understand what needs to get done and how to work with other specialists to ensure that these essential tasks are completed.

One way to frame the course is to look at project and change management as the integration of technical, cultural, and political dynamics and interactions, drawing out more explicitly the critical role of broader human, cultural, and political factors in the change process.
[This orientation will enhance the ability to introduce Assurance Across Life Cycles topics directly into the day-to-day teaching process.]

3.2 MSwA Content Area Two – Risk Management

Analogous MSIS Content Area: MSIS2006.8 Implications of Digitization

Catalog Description MSIS2006.8:

Understanding of the implications of the digitization of data, information, and communications on organizations and society. These implications are examined in regard to ethical issues such as information privacy, accessibility, property, and accuracy. The proliferation of computer crime as well as the legal and regulatory environment is examined. The ramifications of digitization as they affect individuals, organizations, and society. The impacts of globalization, sourcing, technology workforce, and the digital divide are examined.

MSIS Objectives:

Students gain a thorough understanding of the influence of increasing digitization on organizations and society. Digitization of information and the proliferation of global wired and wireless networks are enabling new relationships among organizations, new threats, and new ways of working. Students will examine the characteristics of the information age and explore the implications of emerging ethical concerns such as information privacy, accuracy, property, and accessibility. Students will also examine what constitutes a safe digital environment.

Detailed Topic List:

- *Information systems ethics;*
  - *Ethical issues related to information privacy, accessibility, property, and accuracy.*
  - *Employee monitoring and acceptable use policies.*
  - *Internet enabled vices and the good of society.*
  - *Important laws, regulations, compliance, and treaties including: Sarbanes-Oxley Act; Computer Fraud and Abuse Act, Electronic Communications Privacy Act, Identity Theft and Assumption Deterrence Act, Homeland Security Act; U.S. PATRIOT Act.*
  - *Ethical guidelines for computing professionals.*
  - *Ethical issues related to data retrieval and data mining.*
  - *Globalization and sourcing*
  - *Copyright and intellectual property infringements, the role of peer-to-peer networks*
  - *Mobility, virtualization, and privacy*

  - *Blogging and the media*
- *Security*
  - *How information is compromised including unauthorized access, information modification, denial of service, and viruses.*
  - *Computer crime, cyberterrorism, and cyberwar.*
  - *Computer viruses, worms, Trojan horses.*
  - *Internet fraud, hoaxes and urban legends.*
  - *Spam, adware, and spIM.*
  - *Identity theft and cybersquatting.*
  - *Computer security measures including technological (physical access restraints, firewalls, encryption, and audit controls) and human approaches (legal, effective management, ethics).*
  - *Computer security planning including risk assessment, policy development, implementation, training, and auditing.*

Discussion:

As computing technology and digitization continues to proliferate throughout organizations and society, new issues of legality and ethical behavior have emerged. Since laws don't define ethical behavior, but simply provide societal guidelines for acceptable behavior, a careful examination of the role of digital technologies in shaping ethical behavior is warranted. In addition to ethical issues, the proliferation of digital technologies often creates unforeseen legal dilemmas that existing laws do not sufficiently cover. An examination of current laws, regulations, and treaties provides a foundation for understanding the fuzzy boundary between legal and ethical behavior.

The proliferation of digital technologies throughout society has enabled a plethora of behaviors that are shaping future business environments. A careful examination of various topics including intellectual property issues, computer crime – including viruses, fraud, and hoaxes, technology annoyances – including spam, spyware, cookies, and spIM, employee monitoring, globalization, identity theft, cyberwar and terrorism, and numerous others should be explored. Once a clear understanding of broader organizational and societal implications are explored, professional codes of conduct as well as defining organizational policies for acceptable use should be examined. [Given the direct orientation of this course toward threat and threat understanding, the unique issues associated with software assurance risk, including defects, exploits, and remediations, can be specifically introduced into the learning process.]

3.3 MSwA Content Area Three – Assurance Assessment

Analogous MSIS Content Area: MSIS2006.2 Analysis, Modeling and Design

Catalog Description MSIS2006.2:

Systems development life cycle; analysis and design techniques; information systems planning and project identification and selection, requirements collection and structuring, process modeling, conceptual and logical data modeling, database implementation, design of the human-computer interface and data management, design of the human computer interface (HCI) System implementation and operation, system maintenance, and change management implications of systems.

Students will use current methods and tools such as rapid application development, object-oriented analysis and design, prototyping, and visual development.

MSIS Objectives:

This course provides an understanding and application of system analysis and design processes. Students evaluate and choose appropriate system development methodologies and design a system. Students learn the importance of effective communication and integration with users and user systems. The course emphasizes interpersonal skill development with clients, users, team members, and others associated with development, operation, and maintenance of systems.

Detailed Topic List:

- *Systems development methodologies including life cycle and iterative design models; development phases including systems selection and planning, analysis, logical design, physical design, implementation and operation, maintenance*
- *Techniques for requirements determination, collection, and organization (questionnaires, interviewing, document analysis, observation); joint application design (JAD) and other group approaches (e.g., electronic JAD, computer conferencing); prototyping*
- *Team organization and communication; interviewing, presentation design, and delivery; group dynamics; and leadership*
- *Project feasibility assessment and risk analysis*
- *Design reviews and structured walkthroughs*
- *Systems development life cycle; object-oriented analysis and design; Rapid Application Development (RAD); eXtreme programming; prototyping*
- *Core UML diagrams; principles underlying the widely used object-oriented process models.*
- *Data organization and design: conceptual data modeling; logical data modeling using relational technologies; database definition and manipulation using SQL*
- *Human-Computer Interaction design (depth of focus will depend on how overall curriculum is implemented – see MSIS 2006.9 for key topics)*
- *Software and system quality metrics*
- *Application categories*
- *Software package evaluation and acquisition, open source, managing external relationships and procurement.*

Discussion:

Context of the course in the total curriculum: The analysis of an organization — its users, data, and business processes — and the subsequent design of computer systems to meet business requirements is at the heart of the information systems field. Understanding the processes and techniques used to design and implement information systems is fundamental to managing — identifying, analyzing, designing, implementing, operating, and evolving — technical resources within an organization. This course provides conceptual understanding of "where systems come from" and practical knowledge for managing the system development process.

Philosophy in the selection of topics: In the analysis, modeling, and design of both large and small information systems, it is typical that multiple individuals participate in the process. It is common that analysts work with users, managers, and other analysts to design the system while also working with technical specialists and vendors to implement the required designs. [Given the MSIS orientation toward management data and quantitative analysis, the content related to assurance assessment would provide a value-added fit with the more business-oriented quality assurance processes.] *Effective communication is at the heart of a successful information systems project. To communicate effectively, a structured and disciplined approach to the systems analysis and design process is required.*

Systems design and development is firmly rooted in an organizational context — it is not merely a "technical" or "computer" activity, but a "business" activity. Success requires not only skill in system methodologies and techniques, but also in the management of people and projects. At a very fundamental level, the design and development of organizational information systems involves solving problems and communicating problem diagnoses and solutions to others in a wide range of forums and media. Applying the methods, techniques, and tools used to determine information requirements, and to document these requirements in a thorough and unambiguous form, is fundamental to the success of the project.

In recent years, the object-oriented approach gained the status of a de facto standard that can be used during all phases of the systems development life cycle from business process modeling to coding. [Because of the importance in this course of objective information that is quantitatively derived, the content of the MSwA Assurance Assessment topic area would appear to be an important, value-added area of special interest here.]

3.4 MSwA Content Area Four – Assurance Management

Analogous MSIS Content Area: MSIS2006.3 Enterprise Models

Catalog Description MSIS2006.3:

Provides a process-oriented view of the organization and its relationships with suppliers, customers, and competitors: processes as vehicles for achieving strategic objectives and transforming the organization; process analysis, design, implementation, control and monitoring; processes as a means of achieving compliance; impact on work; the role of enterprise resource planning (ERP), supply chain management (SCM), and customer relationship management (CRM) systems. The process continuum: from structured to unstructured processes: Impact on work practices: The role of systems in transforming organizations and markets; global perspectives.

MSIS Objectives:

Students learn: how to evaluate and understand the role of processes in a competitive environment; how processes integrate the internal functions of the firm and allow the firm to interact with its environment. They are able to recognize, model, and improve processes to achieve efficiency and compliance objectives. They understand the role of ERP, SCM, and CRM systems as components of the enterprise architecture; the impact of automation on work practices; unstructured collaborative and knowledge management processes.

Detailed Topic List:

- *A strategic view of processes; concepts of organizational efficiency and effectiveness*
- *Integrating the functional areas of the organization*
- *Relating processes to the financial, customer, and product-oriented goals of the firm*

- *Process innovation: analysis, modeling and simulation*
- *Business process automation*
- *Using Activity Diagrams and Business Process Modeling Notation (BPMN) for business process modeling*
- *Business Process Modeling tools*
- *Job redesign; impacts of automation on work practices*
- *Achieving security and process compliance*
- *Monitoring and controlling processes*
- *Supply chain management (SCM)*
- *Customer relationship management CRM)*
- *Enterprise management systems (ERP)*
- *The process continuum: from structured to unstructured processes*
- *Collaborative systems*
- *Knowledge management systems*
- *Processes that span the world; global virtual markets.*

Discussion:

The evolution of information systems can be seen as a progression of concerns and competencies involving systems of ever increasing scope and complexity. In the early days, IS focused on individual programs and files; databases were introduced to integrate scattered and redundant files and to manage the data resources of the organization; workflow management and ERP systems were introduced to integrate the functional applications and their data, thus expanding the scope of IS to the total organizational system; supply chain management and customer relationship management systems increased the scope further to a distributed network of organizations and individuals; finally, the forces of globalization and sourcing expand the focus of IS to global networks that operate 24x7 and unite organizations and workers around the world into a virtual system of systems that has vast economic and geopolitical impacts that are beyond current understanding. [Given this orientation, it would seem that the content of the MSwA curriculum would be an extremely valuable building block that could potentially add much more in-depth substance to the current topic. In addition, the global orientation of the MSIS content area toward real-world practice might be something the MSwA curriculum designers should consider for their curricula. There is very good synergy between these two models at this point.] *From this viewpoint, processes can be seen as the glue that binds the organization, its functional areas, and its workers together into a single entity and that link the organization to its global environment.*

The course starts by considering the strategic role of processes. … While strategic advantage may be transitory, most companies need efficient processes to remain competitive. The course then considers issues of organizational transformation and the relationship between organizational structures, processes, and the employee roles. Next, students learn how to develop process maps and design process improvements. The impact of regulations such as Sarbanes-Oxley and Gramm-Leach-Bliley on the controls that must be built into the firm's processes and databases are considered next. [The emphasis on process and practical application of assurance principles is very close to the focus of the MSwA and would allow for an easy integration of content. The fact that the MSwA content would both elaborate and better

focus the learning in this area makes it important to consider an immediate integration of content from these two areas.]

3.5 MSwA Content Area Five – System Security Assurance

Analogous MSIS Content Area: MSIS2006.6 Policy and Strategy

Prerequisites: MSIS2006.1 and MSIS2006.2

Catalog Description MSIS2006.6:

The top management, strategic perspective for aligning competitive strategy, core competencies, and information systems. The development and implementation of policies and plans to achieve organizational goals. Defining the systems that support the operational, administrative, and strategic needs of the organization, its business units, and individual employees. Approaches to managing the information systems function in organizations, including examination of the dual challenges of effectively controlling the use of well-established information technologies, while experimenting with selected emerging technologies. Role of the CIO.

MSIS Objectives:

Students develop an understanding of the strategic use of information technology from a business perspective at the enterprise level. They are expected to understand the internal management of information systems services from the point of view of the CIO and to examine alternative strategies and tactics available to management to achieve goals. Working students and students with post-baccalaureate experience will be able to examine the current and potential impact of information and information technology on all aspects of their position, firm, and industry. Students without experience will be able to understand the strategic information thrust of potential employers.

Detailed Topic List:

- *Relationship between IS and the business*
- *Aligning IT with the cored* [sic] *competencies and strategies of the firm and assess the impacts on organizational competitive position*
- *Translate strategic and IT objectives into operating principles for IS planning*
- *IS planning including infrastructure planning and budgeting*
- *IS implementation*
- *Sourcing vs. insourcing*
- *Interorganizational systems and electronic commerce*
- *IS personnel, structure, and leadership*
- *Risk management*
- *The virtual organization*
- *Implications of globalization.*

Discussion:

Philosophy underlying selection of topics: This course is often taught as a case-based course near the end of the student's MS program. By that time, the student has developed a broad perspective on IS and knows about it at a detailed level. This course, together with the Inte-

grated Capstone course completes the managerial portion of the MSIS program. [The addition of a specific security concentration into the joint Policy and Strategy/Capstone arrangement would allow information students to obtain a specific grounding in the critical area of secure software assurance. As a consequence, the contents of the MSwA System Security Assurance area would be easy to produce and would provide an extremely valuable area of focus, as well as a highly marketable specialization for MSIS students.]

3.6 MSwA Content Area Six – System Functionality Assurance

Analogous MSIS Content Area: None identified

3.7 MSwA Content Area Seven – System Operational Assurance

Analogous MSIS Content Area: None identified

Appendix: Incorporating a Software Assurance Focus into a Typical Information Systems Master of Science in Software Management (MSCIS) Program

The current Master of Science in Software Engineering Management Program at the University of Detroit Mercy is already a hybrid of two disciplines. Those disciplines are embodied in the recommendations of the AIS's MSIS 2006 model for graduate information systems programs and the process areas of the Software Engineering Body of Knowledge (SWEBOK). Therefore, the current curriculum can be easily modified to capture the first five (Section 1) core body of knowledge areas of the MSwA reference curriculum.

Core Courses

CIS 5010 Introduction to Information Systems – Operating System Concepts

Directly satisfies MSwA element "Computing Foundations" as well as prerequisite requirements of MSIS2006.

CIS 5100 Object Orientation – Threat Modeling

Directly satisfies MSwA element "Risk Management" and some aspects of "Assurance Assessment"; satisfies MSIS element 2006.2, "Analysis Modeling and Design."

CIS 5200 Secure Specification

Directly satisfies MSwA element "Assurance Across Life Cycles" as well as some aspects of "Assurance Management and Assurance Assessment"; satisfies MSIS element 2006.5, "Project and Change Management."

CIS 5300 Secure Software Assurance

Directly satisfies MSwA element "Assurance Assessment" as well as some aspects of "Assurance Management"; satisfies MSIS element 2006.2, "Analysis Modeling and Design."

CIS 5400 Secure Life Cycle Management

Directly satisfies MSwA element "Assurance Management" as well as some aspects of "Assurance Across Life Cycles"; satisfies MSIS element 2006.3, "Enterprise Models," and 2006.6, "Policy and Strategy."

Additional Elective Courses (5)

CIS 5050 Project Management

Directly satisfies MSIS 2006.5 "Project and Change Management."

CIS 5250 Secure Software Construction

Directly satisfies MSwA element "System Functionality Assurance."

CIS 5350 Metrics and Models for Software Management

Directly Satisfies MSwA element “Assurance Assessment”; satisfies MSIS element 2006.6, “Analysis Modeling and Design.”

CIS 5530 Human Factors in IT Security

Directly satisfies MSIS element 2006.9, “Human Computer Interaction.”

CIS 5540 Post-Release Sustainment

Directly satisfies MSwA element “System Operational Assurance.”

CIS 5570 Network Security and CIS 5590 Advanced Network Security

Both satisfy MSIS element 2006.3, “Data Communications and Networking.”

CIS 5700 Information Assurance Principles

Directly satisfies MSwA element “System Security Assurance”; satisfies MSIS element 2006.8, “Implications of Digitization.”

CIS 5580 System Forensics, CIS 5750 Information Assurance Technologies, and CIS 5790 Information Assurance Processes

Directly satisfy MSwA element “System Security Assurance”; potentially satisfies MSwA element “System Operational Assurance”; satisfies MSIS element 2006.8, “Implications of Digitization.”

CIS 5910 Information Security Audit

Directly satisfies MSwA element “Assurance Assessment and System Security Assurance”; satisfies MSIS element 2006.6, “Analysis Modeling and Design.”

References

[Abran 2004]
Abran, Alain & Moore, James W. *Guide to the Software Engineering Body of Knowledge (2004 Version)*. IEEE Computer Society, 2004.

[Ardis 1989]
Ardis, M. & Ford, G. *1989 SEI Report on Graduate Software Engineering Education* (CMU/SEI-89-TR-21, ESD-TR-89-29). Software Engineering Institute, Carnegie Mellon University, 1989. http://www.sei.cmu.edu/library/abstracts/reports/89tr021.cfm

[Banker 2004]
Banker, Rajiv D. & Kauffman, Robert J. "The Evolution of Research on Information Systems: A Fiftieth-Year Survey of the Literature of *Management Science*." *Management Science 50*, 3 (March 2004): 281-298.

[Bishop 2006]
Bishop, Matt & Engle, Sophie. "The Software Assurance CBK and University Curricula," 14-21. *Proceedings from the Tenth Colloquium on Information Systems Security Education*, University of Maryland University College, MD, June 2006.

[Bureau of Labor Statistics 2009]
Bureau of Labor Statistics. *Occupational Outlook Handbook – 2010-2011 Edition.* http://www.bls.gov/oco/ocos258.htm (2009).

[DHS 2003]
U.S. Department of Homeland Security. *The National Strategy to Secure Cyberspace.* U.S. Department of Homeland Security. http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf (2003).

[Ford 1991]
Ford, G. *1991 SEI Report on Graduate Software Engineering Education* (CMU/SEI-91-TR-002, ESD-TR-91-002). Software Engineering Institute, Carnegie Mellon University, 1991. http://www.sei.cmu.edu/library/abstracts/reports/91tr002.cfm

[Goertzel 2007]
Goertzel, Karen Mercedes; Winograd, Theodore; McKinley, Holly Lynne; Oh, Lyndon; Colon, Michael; McGibbon, Thomas; Fedchak, Elaine; & Vienneau, Robert. *Software Security Assurance: A State-of-the-Art Report (SOAR).* U.S. Information Assurance Technology Analysis Center (IATAC) and Data and Analysis Center for Software (DACS), Department of Defense. http://iac.dtic.mil/iatac/download/security.pdf (2007).

[Gorgone 2006]
Gorgone, John T.; Gray, P.; Stohr, E. A; Valacich, J. S.; & Wigand, R. T. "MSIS 2006: Model Curriculum and Guidelines for Graduate Degree Programs in Information Systems." *Communications of the Association for Information Systems 17*, 1, Article 1 (Jan. 2006): 2-75.

[Impagliazzo 2002]
Impagliazzo, John & Gorgone, John T. "Professional Accreditation of Information Systems Programs." *Communications of the Association for Information Systems 9*, 1, Article 3 (Aug. 2002): 50-63.

[Mead 2008]
Mead, Nancy R.; Shoemaker, Dan; & Ingalsbe, Jeffrey. "Integrating Software Assurance Knowledge into Conventional Curricula." *STSC Crosstalk 21*, 1 (Jan. 2008): 16-20.

[Mead 2010]
Mead, Nancy R.; Allen, Julia H.; Ardis, Mark; Hilburn, Thomas B.; Kornecki, Andrew J.; Linger, Richard; & McDonald, James. *Software Assurance Curriculum Project Volume I: Master of Software Assurance Reference Curriculum* (CMU/SEI-2010-TR-005, ESC-TR-2010-005). Software Engineering Institute, Carnegie Mellon University, 2010.
http://www.sei.cmu.edu/library/abstracts/reports/10tr005.cfm

[PITAC 2005]
President's Information Technology Advisory Committee. *Cybersecurity: A Crisis of Prioritization.* Executive Office of the President, National Coordination Office for Information Technology Research and Development, 2005.

[Redwine 2006]
Redwine, Samuel T., ed. *Software Assurance: A Guide to the Common Body of Knowledge to Produce, Acquire and Sustain Secure Software, Version 1.1.* U.S. Department of Homeland Security, 2006.

[Redwine 2008]
Redwine, Samuel T. *Toward an Organization for Software System Security Principles and Guidelines.* The Institute for Infrastructure & Information Assurance at James Madison University, 2008.

[SIT 2009]
Stevens Institute of Technology. *Graduate Software Engineering 2009 (GSWe2009): Curriculum Guidelines for Graduate Degree Programs in Software Engineering.* Stevens Institute of Technology.
http://www.gswe2009.org/fileadmin/files/GSwE2009_Curriculum_Docs/GSwE2009_version_1.0.pdf (2009).

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	February 2011	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Integrating the Master of Software Assurance Reference Curriculum into the Model Curriculum and Guidelines for Graduate Degree Programs in Information Systems	FA8721-05-C-0003

6. AUTHOR(S)

Dan Shoemaker, Nancy R. Mead, Jeff Ingalsbe

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2011-TN-004

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116	

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

Training personnel to assure the secure development, sustainment, and acquisition of software code is a national priority. However, in the secure software domain, there is no single, commonly accepted point of reference to direct software assurance education and training. In response to this problem, the CERT® Program at Carnegie Mellon University's Software Engineering Institute recently led the development of a Master of Software Assurance (MSwA) Reference Curriculum. This report examines how the recommendations of the MSwA Reference Curriculum might be integrated into the model curriculum recommendations for a Master of Science in Information Systems (MSIS). This integration is important because IS programs constitute a key portion of computer education programs in the United States. The report describes the content areas of the MSIS curriculum that appear to be most relevant to secure software assurance practice. It also details the places in the current MSIS curriculum model where recommendations of the MSwA Reference Curriculum appear to fit. In addition the report explains how those recommendations can be integrated into a conventional MSIS curriculum and provides an example of an existing MSIS curriculum that embodies them.

14. SUBJECT TERMS	15. NUMBER OF PAGES
software assurance education, information systems education, graduate curricula	31

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL